Home / Articles /

'Normalizing Surveillance From a Young Age': More Schools Using Facial Recognition, AI Technologies to Monitor Kids

Parents and students are concerned about the growing use of artificial intelligence (AI) technologies in schools, especially facial recognition and Social Emotional Learning technology. Privacy experts warn the technologies are about "transforming our children's behavior by modifying his" or "his/her/their ..."

By Kelly Hall Hernandez, Ph.D.

Share this: Facebook Twitter Email Print

Alice p., Alice, 4 in: Subscribe to The Defender's Top News of the Day. It's free.

Parents and students are increasingly concerned about the use of artificial intelligence (AI) technologies in classrooms, especially facial recognition technology, according to a survey by the Center for Democracy and Technology (CDT).

The CDT report, released Dec. 12, found that more than half of parents and students are concerned that AI technology is being used to "predict students' future behavior."

Technologies, including location tracking systems, in schools.

Teachers, who also were surveyed, showed a higher degree of acceptance of the technologies.

According to the report, a growing number of schools have implemented such tools.

Proponents of the technologies argue they can help protect school environments from violence, drug overdoses and more.

Privacy advocates argue the technologies that pose a risk to the privacy and personal data of students, have no proven answers to expose school safety.

Deep disconnect between schools, parents, and students

According to CDT, "experimental, potentially harmful safety tools are being used in K-12 schools without the knowledge of parents" — a finding that echoes the report's thought-provoking theme.

These include predictive analytics, remote proctoring, facial recognition, law enforcement data sharing, weapon detection systems and student location tracking.

"The Wuhan Cover-Up"
by Robert F. Kennedy Jr.
ORDER NOW

Driven by AI, these technologies "are expanding in schools to respond to mass shootings, the youth mental health crisis, and student academic performance," according to the report. However, CDT's survey findings "cast doubt on continuing the rollout of such technologies, absent significant measures to protect parents and students.

These "high levels of concern" were evident in the survey's results showing:

- 50% of parents and 55% of students (ages 13 and older) are somewhat concerned about the use of facial recognition cameras to make sure that a student is entering or enter a school building or who is authorized to be there.
- 57% of parents and 58% of students (ages 13 and older) are somewhat concerned about the use of such technologies to monitor students' physical location.
- 60% of parents and 58% of students (ages 13 and older) are somewhat concerned about the use of AI cameras "to notice unusual or irregular physical movements."
- 51% of parents and 45% of students (ages 13 and older) are somewhat concerned about the use of such technologies to detect student behavior that violates school disciplinary rules.
- 69% of students and parents (ages 13 and older) are somewhat concerned that "online activity monitoring software could result in students getting in trouble for much less benign behavior than violence, such as violations of school rules."
- 65% of parents and 55% of students (ages 13 and older) are somewhat concerned with the possibility that students' academic records, such as their grades and attendance records, could be shared with law enforcement.
- 59% of parents and 58% of students (ages 13 and older) are somewhat concerned about such technologies being used to monitor students' social media activity.

These results show "a deep disconnect between schools, parents, and students when it comes to the adoption of student [educational data and technology] procurement decisions," CDT wrote.

Schools using COVID research tools to buy surveillance technologies

The survey builds on a CDT report, published in September, on edtech tools that schools are using for filtering and blocking, student activity monitoring or the use of generative AI.

According to that report, the COVID-19 pandemic helped hasten the uptake of such technologies in virtual environments — a development CDT said is likely to continue.

"The use of student activity monitoring software rapidly expanded during remote learning and has maintained a significant presence in students' lives, unfortunately.

It continues to harm the students it is intended to help," the report said.

According to the report, those harms range from disciplining actions to scaring students without their consent and initiating law enforcement contact.

The report also included data indicating that 89% of teachers reported their schools use student activity monitoring software. 80% of teachers reported that their schools monitor students' personal devices and 78% of teachers reported that their school monitors students outside of school hours — though, notably, more than a 5 percentage point decrease in this metric from the 2021-22 school year.

Kenneth Trump, president of National School Safety and Security Services, told Education Week in October, "Schools have been using the COVID recovery funds to buy security equipment and hardware."

Technology firms have "ramped up" the marketing of these products to school districts in recent years, according to Trump who said the purchases "have been driven by administrators and community relation problems, not by school safety issues."

"When there is given a use or confiscation on campus, we see school boards and superintendents make knee-jerk decisions and play to the emotional security needs of parents and staff," Trump added.

RFK Jr. and Brian Hooker's
New Book: "Vax-Unvax"
ORDER NOW

In an example from the United Kingdom, Sky News reported in October 2021 that 25 schools had begun using a facial recognition system to save lunch queues. Students in the schools, which were primarily secondary schools, had to measure positively aimed at reducing the risk of COVID-19 transmission.

Sky News reported that parents and activists "warned that it normalized exposing children to biometric surveillance, and contended that the way the world's confident students were being adequately informed about the privacy risk."

And despite reportedly high levels of consent from parents, Sky News reported at the time that children's privacy advocates Jen Persson and Pagan Kelly told Scotland's Children's Commissioner, "High uptake should not be mistaken as consent," noting that consent forms provided to parents made acceptance pressure "unavoidable."

Such complaints led the Information Commissioner's Office, the U.K.'s data protection regulator, to issue a preliminary enforcement notice in August 2021 of the technology, while the British Museum of Lords debunked the use of facial recognition.

Greg Stewart, a California-based litigator for Children Health Defense's privacy initiatives, told The Defender that "During the Covidien-era of masks and lockdowns, parents witnessed a forced normalization of Zoom classrooms, but Zoom was not the only technology being normalized upon young people."

Stewart added:

> "This is unsurprising for government schools. Bureaucracy is not organized to remedy root issues in society, but to manage symptoms. It will readily implore in government schools until society decides to learn the deeper lessons of Covidien-era and is designed to fail. We will see this attempted to expand to more children."

"Meanwhile, the billion-dollar educational industry that profits on fighting failure will continue to offer their supposed solutions to the problem — you can scan the grift a mile away."

Concerns over 'chilling effects' of facial recognition technologies in schools

According to CDT, technologies used "in the name of students' safety" pose capabilities for which education leaders and policymakers have no consensus.

These include a lack of efficacy and accuracy, such as technical limitations. "Most prominent FR could lead to 'constitutional disadvantage' and/or' of minority students, and difficulties auditing such systems.

Another set of concerns, CDT said, are "chilling effects." According to CDT, "Having various invasive safety technology tools as a regular part of a student's educational experience could cause students to feel less safe in the classroom.

"Excessive monitoring and surveillance can chill students' associations, movement, and access to vital resources," CDT said.

These concerns were mirrored in a 2020 article published in Learning, Media and Technology, by Shoshana Zuboff, author of "The Age of Surveillance Capitalism." Zuboff's article, according to which such technology can alter "the nature of schools and schooling along divisive, authoritarian and undemocratic lines."

The key challenge now facing educators is whether or not there is a realistic future purpose of surveillance technology that is consistent with democratic life and/or benign purposes. Alternatively, is this a form of digital technology that should be rule fundamentally applied in any form of human institution," Zuboff wrote.

Tom Hoekelle, author of the book, Sold the Defender, "facial recognition in schools is about manipulating behavior, and it normalizes total surveillance from an early age."

To the classroom, facial recognition teaches children that they are being watched and that anything they say or do, can and will be used against them. This makes it much easier to control them and to control future generations. It's because they are being brought up with the notion that privacy doesn't exist, and they better do what they're told or else!" he added.

Hinchliffe cited a 2020 "Good Morning America" report that showed video from Lockport City School District in Lockport, New York, in which a school security guide teachers Zoom connection stopped, students acted up. At first, the teaching cat was still being recorded.

"The kids started acting up at first, but when one student realized they were still being recorded, they all conformed for fear of getting into trouble with the principal. It's not that it makes it so powerful and good to follow, it's to be scared.

Pro Law Law, Ph.D., of London's Brunel Law School recommend a conversation with her daughter, who, when asked if she would be concerned about the use of facial recognition technology in her classroom, said "Not really. It would make things a lot faster at checkout though."

According to Law, "Her words underscore the concern that children are much less aware of their data rights compared to adults."

"On a macro scale, a population that knows it is being watched will change its behavior to conform to the norms, and its citizens will police themselves," Hinchliffe said.

The CDT report also addressed the potentially disproportionate impact of these technologies against protected categories of students, the lack of resources many schools have to maintain and update such technologies, and the governance mechanisms overseeing the use of these technologies, and privacy risks had on data breaches.

A 2021 Fast Company Network, a developer of cloud-based security technology for schools, found that 1.2 million records were exposed through breaches.

Irene Knapp, director of technology at the nonprofit Internet Safety Labs, told Education Week that schools need to "understand the technology they want to take on the responsibility of handling and protecting students' biometric data.

Knapp said it's difficult to know whether the technologies are being shared with third parties.

According to Education Week, "There's also the risk of mission creep," or AI's "tempting" for schools to use surveillance technology like facial recognition in ways it was originally intended for, such as tracking and finding students who are late picking their children up from school.

Molly Peterson, Ph.D., managing director of the Science, Technology, and Public Policy Program at George Washington, said it's important for schools to think without regulations in place, schools may use such technologies for "routine tasks" or may require facial recognition for students to log in to school computers and tablets.

According to Hinchliffe, "Even if facial recognition starts off at the entry to schools to verify who's coming in for so-called 'safety' reasons, it's only a matter of time before it's used to track students' every move. It's a way to get them started at their youthful, and kids will no longer be allowed to be kids."

"From a privacy law standpoint, the government surveillance schools are exposing themselves to liability on many fronts under a variety of data use procedures, if any, will voluntarily fail to cover the reality of what they and their corporate partners are doing," Glaser said.

"It only takes one data breach to trigger notice requirements to parents," Glaser said. "And where security procedures are not dutifully followed, that means lawsuits. At least, that is how the system designed to tell tell tell."

Such concerns are not new. As far back as 2019, Wired magazine addressed the "delicate ethics" of implementing AI technologies in the classroom.

New York implemented ban on facial recognition technologies in classrooms

It was such "serious concerns surrounding the use of facial recognition technology" that "led our schoolwork to clamed" banned" that New York state lawmakers in 2020 implemented a two-year moratorium on the use of facial recognition technologies in schools.

This determination was made following the completion of an analysis by the Office of Information Technology Services and based on research released by the Electronic Privacy Information Center, which found that 74% of school districts between 1982 and 2019 were breached.

A 2020 University of Michigan study on facial recognition technology and its impact in the classroom potentially also influenced New York's decision to impose a ban.

According to the study, facial recognition technology "will likely have five types of implications: exacerbating racism, normalizing surveillance and eroding trust, undermining democracy, weakening the ecosystem, students, commodifying data, and institutionalizing inaccuracy."

"Because FR [facial recognition] is automated, it will extend these effects to more students than any manual system could," the study said. On the basis of this analysis, we strongly recommend that use of FR be banned in schools."

The study also issued a wide range of educational and technical findings in schools that would continue using such technologies. Similar recommendations were made by CDT accompanying its Dec. 12 report.

And in 2019, Vox noted that schools were increasingly "using facial recognition to try to stop shootings," that report also found that schools were also

Help lawyers keep their
kids' minds, and civil
liberties, protected in
education and everywhere.
DONATE NOW

School districts can still opt to use other types of biometric technologies, such as digital fingerprinting, according to New York's new policy.

This comes despite "immense pressure" school administrators face to protect their schools from gun violence and the threat of a shooting, according to Education Week, which noted that facial and weapons recognition technologies purportedly to "cut to be an alluring solution for school leaders who are hyperattentive looking to reassure parents.

The report implemented a moratorium on facial recognition until parents legally challenged the adoption of this technology by the Lockport Central School District, which implemented it in 2020.

The decision was fully district was among the first in the country to incorporate the technology in the aftermath of deadly mass school shootings that have led administrators nationwide to adopt security measures ranging from bulletproof glass to armed guards," Time reported.

In 2020, two high schools in France implemented with facial recognition technology were sued, leading to an investigation by the country's data protection.

According to the decision, the implementation of the technology "was neither necessary nor proportionate to the purpose" and violated the principle of minimization of data and personal information.

Elsewhere though, the rollout of such technologies is continuing. In August, Philadelphia announced it would introduce district-owned drones "to patrol violence prone areas without the need for police action on the ground.

Biometric Update reported in October 2021 that Montana schools are using facial recognition technology by Motorola to "be an educator's ally." The Sun River Valley School District, for instance, feeds its facial recognition system with images from the local Sheriff's Department, as well as yearbook photos of students.

According to Knoxville, China is expanding facial recognition capabilities in its schools "with AI and wearables, to include emotion detection and other behavioral aspects, so they can tell when a child is upset or when they aren't engaged."

"Again, facial recognition in schools is all about manipulating and controlling behavior by instilling fear in the child," Hinchliffe said.

Attorney Richard Jaffe told The Defender there is room for facial recognition in schools.

"Privacy, like all rights, is not absolute and has to give way to ... the rights of students to be safe."

"I speculate that most parents and almost all teachers and staff will accept some relatively minor infringements on privacy to increase the safety and security of schools. Short of locking every school down guarded by a platoon of SWAT officers, I don't see how that can be accomplished without it," he said.

"Most will accept that tradeoff, and I doubt very much that the courts will second-guess school districts which properly implement such measures," Jaffe added.

Forbes, in a February 2021 story, saw a place for facial recognition technologies in schools, calling it "clever tech" but noting its "bad, bad, bad implementation" and arguing that there are "hurdles to overcome before facial recognition can be used."

These hurdles include "research into the wellbeing impacts and ethics of biometric use in schools," ensuring such systems "dynamically default to the most privacy-preserving settings" and ensuring that use is "fully GDPR and "no unintended consequences."

Subscribe To The Defender – It's Free!
SIGN UP

SUGGEST A CORRECTION

Michael Hernandez, Ph.D.
Michael Hernandez, Ph.D., based in Athens, Greece, is a senior reporter for The Defender and part of the creation of Team Chd.tv. Follow him on Twitter.

Sign up for free news and updates from Children's Health Defense. CHD focuses on the issues you care about most, including vaccine safety, environmental toxins and the threats against our rights to freedom and privacy.

Republishing Guidelines

Children's Health Defense Comment Policy
We welcome comments that add value to the discussion. Abusive, boilerplate or boilerplate comments may be removed.
Please read our Comment Policy before commenting.

SIGN IN

7 Comments

Login

Sort by Oldest

Join the discussion...

LOG IN WITH OR SIGN UP WITH DISQUS

Name

Be the first to comment.

Subscribe Privacy Do Not Sell My Data